#	Topics	Responsible person/ responses
1	Identity & Access Management • Access grant and revocation for terminated employees • Privilege utility programs, privileged access management and protection of access control system	SOP IT003 outlines Cogstate role-based access controls and procedures for on-boarding/offboarding of personnel. SOP IT013 and SOP IT003 outline system administrator accounts and access granting. Cogstate's Human Resources submits a ticket with the IT Department with the new employee's information. IT will register the employee in Cogstate ticket tracking system to track the employees access throughout their employment at Cogstate. IT will request the hiring manager to approve the access to be granted to the new employee, including hardware requirements. Access and hardware will be granted by IT upon hiring manager's documented approval. Upon a user's termination at Cogstate, Cogstate's Human Resources submits a ticket with the IT Department. IT documents deactivation of access granted from the employees onboarding documented when the employee was hired, in addition to any access granted during their term. Access to high level systems and elevated access are documented following the same steps for employee access. Multi-factor authentication is utilized when available. Upon termination of user with elevated access, system passwords are rotated where employee was granted access prior.
2	Network Security • Network Diagrams, Firewalls, VPN, etc. • External Vulnerability tests, Penetration tests, etc. Remote access, VPN requirements (MFA, etc.)	SOP IT003 & SOP IT013 outline Cogstate network infrastructure. Cogstate utilizes network segmentation and firewalls are implemented, patched, monitored and maintained routinely. VPN access is role-based, available to all domain users. Network diagrams are maintained and updated upon infrastructure changes. Annual penetration testing is performed by 3rd party vendor, results are reviewed by company stakeholders. Remote access is role-based controlled. System administrator accounts are control and are enforced MFA.

3	Human Resource and Governance • Hiring and termination practices • Background check procedures Information Security group Security Awareness activities Independent review of Information Security program	Hiring: All candidates go through an interview process. When the hiring team selects the best candidate, the information is submitted to the department head and CEO for approval to move forward with hiring. After receiving approval, HR completes the offer letter and agreements. After the candidate accepts, HR initiates the onboarding process. Terminations: For voluntary and involuntary terminations, the manager of the employee informs HR of the decision. HR coordinates with the other stakeholders (IT, Payroll, etc.) of the process to complete the necessary offboarding steps such as deactivating the user's access. Background checks: Background checks are conducted for full time, part time and temporary staff using a third-party background check company. The background check results are reviewed by HR on a case-by-case basis. If/when necessary, Legal is included for further review. Cogstate Security and Privacy Committee meet quarterly to discuss and review Information Security program. Information is provided to employees regarding best practices of security awareness.
4	Physical Security • Physical intrusion monitoring, detection and response • Visitor and Employee access, CCTV coverage	Cogstate US offices are held within an office building which utilizes security personnel 24/7 monitoring and CCTV coverage. Security badges are mandatory and prevents unauthorized intrusion. Visitors are always escorted by a Cogstate staff.
5	Endpoint Security • Endpoint security, Server security • Patch Management Encryption of data at rest and in transit Antivirus solutions	Patch Management is performed monthly (unless if vulnerability is exposed) and documented in centralized ticketing system. Endpoints hard drives are encrypted and antivirus is controlled from a central server.

	DLP solutions, Internet content filtering solutions Central audit logging capabilities in place for various types of audit logs	Cogstate utilizes DLP services from 0365 retention polices to prevent loss of data. Firewalls are in place in all Cogstate offices and in Cloud infrastructure. Every Cogstate system has audit logging enabled and is capable of reporting.
6	Business Continuity and Disaster Recovery • BC/DR controls in place • BC/DR test plans and test results BIAs and relevant RTOs/RPOs Physical and environmental controls in place for ensuring that critical systems and supporting infrastructure remains available	Cogstate has a Business Continuity and Disaster Recovery Plan in place. This prepares Cogstate event of extended service outages that can disrupt business operations caused by factors beyond its control. BC/DR tests are performed annually and are tested against set RTO and RPOs for given scenarios and ultimate RTO and RPO's for the company as a whole.
7	Asset Management • Software and Hardware asset management • Disposal of assets	Cogstate utilizes a System Asset List to define Physical, network, software, hardware and security controls pertaining to each asset. Hardware asset management is held in Cogstates Asset Software (WASP Mobile assets). Each Cogstate asset is given a unique ID, asset assignment is documented. Disposal of assets are performed through a vetted Cogstate Vendor who produces certificate of destruction for disposed devices.
8	Third Party Management • Due diligence of third parties while onboarding and offboarding Ongoing Monitoring practices	Cogstate has a Vendor management process in place (SOP ADM 006). All new vendors are vetted through the evaluation process and are required to complete QMS and IT infrastructure and security questionnaires, which are then reviewed by Cogstate SMEs. An audit (onsite or virtual) may follow depending on the responses. Vendors undergo periodic evaluations as per the SOP. Unsatisfactory vendor performance will be put on notice and may be discontinued if poor performance persists.
9	Incident Response • Assessment and classification of incidents • Incident tracking and remediation	Cogstate utilizes audit logs for all systems/applications, which are stored off-site in a cloud bases platform. Administrators are only able to access

		Any incidents would be elevated to John Glueck, General Counsel JGlueck@cogstate.com 203-915-4941; Cogstate's designated Chief Privacy Officer would also be notified at privacy@cogstate,com. Cogstate has established a comprehensive set of policies to ensure we provide appropriate notice in the event of any privacy incident/breach of confidential data, including a comprehensive Security Incident Response Plan which details a clear process for dealing with security incidents, including but not limited to: discovery and identification; containment, analysis and eradication, recovery, and breach notification and post incident activities.
10	Data Privacy • Protection of personal data • Compliance to local regulations (GDPR, etc.)	Depending on what products/ services are being provided by Cogstate for any given clinical trial studies, Cogstate may receive subject identifying information. Cogstate is committed to the privacy and information security principles that undergird the GDPR and other similar data protection regulations. Those principles include: lawfulness, fairness, and transparency; purpose limitation; data minimization (or in HIPAA Privacy Rule terms the "minimum necessary" principle); accuracy; storage limitation; integrity and confidentiality; and accountability. Cogstate has established a comprehensive set of policies to ensure we comply with the requirements of applicable data protection regulation, including where applicable the GDPR and HIPAA. The policies include the standards by which Cogstate sets guidance for employees with regard to the privacy and security of individually identifiable information. Additionally, Cogstate, Inc. (Cogstate's US subsidiary) complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Cogstate, Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles.
11	Cloud Security • Cloud management controls • Encryption of stored data • Protection of scoped data	Cogstate utilizes role-based access systems to ensure proper access is deployed throughout cloud infrastructure. Data is encrypted throughout transmission utilizing TLS 1.2 with 256-bit encryption. Data at rest is encrypted with 256-bit AES encryption.

12	Application security • SDLC practices • Protection of source code and production data	SOP IT 002 outlines the Design and Development Process. This document provides instructions for software development life cycle for all systems/applications developed in Cogstate. This procedure applies to all staff involved in all stages of software development life cycle. Source code is managed from the Engineers. This source code management controls different stages of source code and directly relates to versioned software.